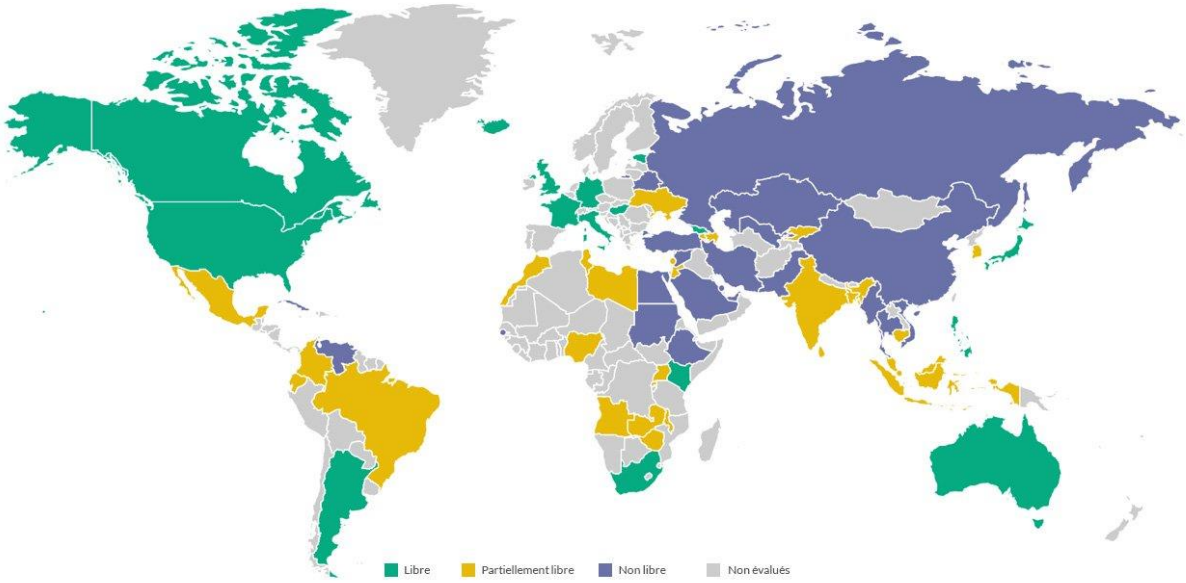
La liberté du Net en 2017



Manipuler les réseaux sociaux pour affaiblir la démocratie

Principaux constats

- La manipulation en ligne et les tactiques de désinformation ont joué un rôle important lors des élections dans au moins 18 pays cette année, y compris aux États-Unis.
- Les méthodes de désinformation ont contribué à faire de cette année la 7ème année consécutive où la liberté sur internet est globalement sur le déclin, auxquelles on peut ajouter l'augmentation des perturbations des service d'accès à internet sur mobile ainsi que le nombre croissant d'attaques physiques et techniques contre des défenseurs des droits de l'homme et médias indépendants.

- Un nombre record de gouvernements a restreint les services internet mobiles pour des motifs politiques ou des raisons de sécurité, souvent dans des régions peuplées par des minorités ethniques ou religieuses.

- Pour la troisième année consécutive, la Chine est le pire détracteur de la liberté en ligne, suivie par la Syrie et l'Éthiopie.
-

Des gouvernements partout dans le monde ont augmenté de manière drastique leurs efforts pour manipuler l'information sur les réseaux sociaux durant l'année passée. Les régimes chinois et russes ont été les premiers à faire appel à des méthodes sournoises pour détourner les discussions en ligne et se débarrasser de toute dissidence, il y a déjà plus d'une décennie, mais ces pratiques sont depuis devenues mondiales. De telles interventions, menées par l'État, sont une menace importante pour internet et sa notion de technologie libératrice.
La manipulation des contenus en ligne a contribué faire de cette année **la septième année consécutive où la liberté d'internet est en chute**, tout comme l'augmentation des perturbations des service d'accès à internet sur mobile et le nombre croissant d'attaques physiques et techniques contre des défenseurs des droits de l'homme et médias indépendants.
Presque la moitié des 65 pays évalués dans *La liberté du Net 2017* (*Freedom on the Net 2017*) ont vu un déclin pendant la période d'analyse, alors que seulement 13 d'entre eux ont fait des avancées, mineures pour la plupart. Moins d'un quart des utilisateurs réside dans des pays où internet est considéré comme « libre », c'est-à-dire sans obstacles majeurs pour y accéder, sans restrictions onéreuses de contenus, ou violations sérieuses des droits des utilisateurs, sous forme de surveillance illimitée ou de répercussions injustes en cas d'expression légitime.

L'utilisation d'intox, de comptes automatisés tenus par des Bots, et d'autres techniques de manipulation ont tout particulièrement attiré l'attention aux États-Unis. Si l'environnement en ligne du pays est resté libre, il a été perturbé par une prolifération de fausses informations, de discours partisans controversés, et par le harcèlement agressif de plusieurs journalistes, à la fois pendant et après la campagne d'élections présidentielles.

Les efforts en ligne de la Russie pour influencer les élections américaines se sont révélés vrais, mais les États-Unis ne sont pas les seuls dans ce cas. Des tactiques de manipulation et de désinformation ont joué un rôle important dans les élections dans au moins 17 autres pays l'année passée, empêchant les citoyens de choisir leurs dirigeants en se basant sur des informations factuelles et des débats authentiques. Si certains gouvernements ont cherché à appuyer leurs intérêts et augmenter leur influence à l'étranger, comme dans le cas des campagnes de désinformation russes aux États-Unis et en Europe, ils utilisent la plupart du temps les mêmes méthodes au sein de leurs frontières pour maintenir le pouvoir.

Le Venezuela, les Philippines et la Turquie font partie des 30 pays où le gouvernement a employé des armées de « faiseurs d'opinion » pour diffuser les idées du gouvernement, mettre en place leurs programmes, et contrer les critiques du gouvernement sur les réseaux sociaux. Le nombre de gouvernements qui ont essayé de contrôler les discussions en ligne de cette façon a augmenté tous les ans, depuis que Freedom House a commencé, en 2009, à analyser ce phénomène de façon systématique. Mais au cours des quelques dernières années, cette pratique est devenue beaucoup plus répandue et sophistiquée, avec des bots, des créateurs de propagande et de faux centres d'information qui exploitent les réseaux sociaux et utilisent des algorithmes pour s'assurer d'une haute visibilité et une intégration fluide avec des contenus fiables.

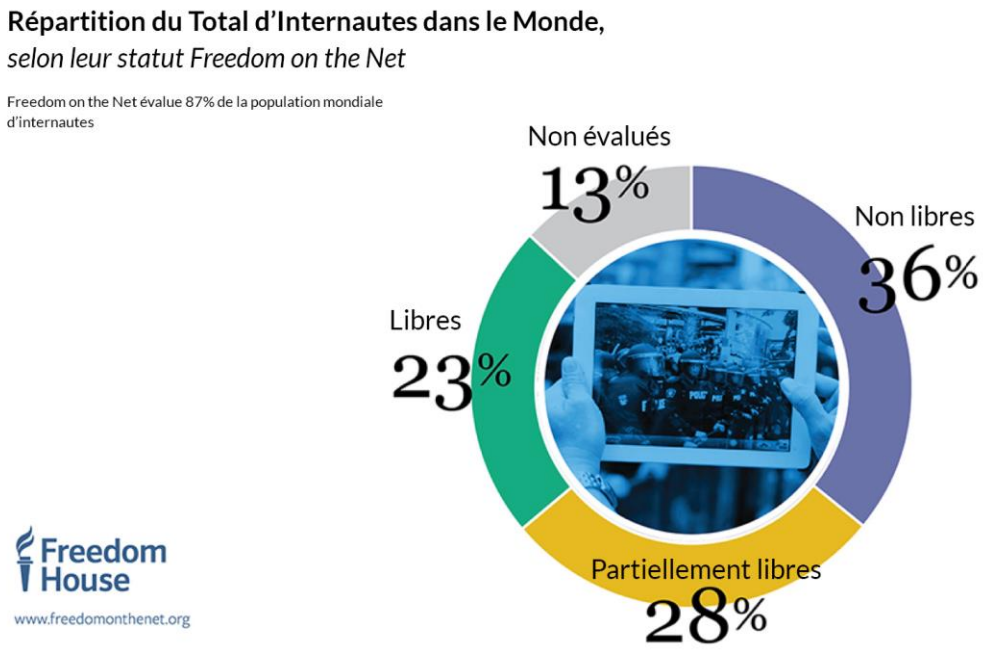
Contrairement aux méthodes de censure directes, comme le blocage de certains sites, ou les arrestations selon les activités internet, la manipulation de contenus en ligne est plus difficile à détecter. Elle est aussi beaucoup plus dure à combattre, de par sa nature étendue et à cause du nombre de personnes et bots employés à ces fins.

Les effets de ces techniques (qui se répandent rapidement) sur la démocratie et l'activisme civique sont potentiellement dévastateurs. La fabrication d'un faux soutien populaire sur les réseaux sociaux crée une boucle fermée dans laquelle le régime s'auto-soutient, laissant les groupes indépendants et les citoyens ordinaires sur la touche. Et en entretenant la fausse idée que la plupart des citoyens les soutiennent, les autorités parviennent à justifier la répression de l'opposition politique et à effectuer des changements antidémocratiques de lois ou d'institutions sans organiser de véritable débat. Il est inquiétant de constater que les tentatives de manipulation sur les réseaux sociaux, sponsorisées par l'État, sont souvent associées à des restrictions plus larges concernant les médias d'informations, pour empêcher l'accès à des informations objectives et rendre les sociétés plus vulnérables à la désinformation.

Réussir à trouver une parade contre la manipulation de contenus et restaurer la confiance en les réseaux sociaux sans affaiblir internet et la liberté de la presse prendra du temps, des ressources et de la créativité. Les premières étapes de ce processus doivent inclure l'information et l'éducation du public, pour apprendre aux citoyens à repérer les informations et commentaires faux ou trompeurs. De plus, les sociétés démocratiques doivent renforcer leurs lois pour s'assurer que la publicité politique soit au moins aussi transparente en ligne qu'elle l'est hors ligne. Et les entreprises technologiques doivent faire leur part en réexaminant les algorithmes à l'origine du tri des informations, et être plus proactives en désactivant les Bots et les faux compte utilisés à des fins antidémocratiques.

En l'absence d'une campagne complète pour traiter cette menace, les techniques de manipulation et de désinformation pourraient permettre aux régimes autoritaires

modernes d'étendre leur emprise et leur influence tout en affaiblissant la confiance des utilisateurs envers les médias en ligne et l'ensemble d'internet.



Autres tendances clés

La liberté du Net 2017 a identifié cinq autres tendances qui ont significativement contribué au déclin mondial de la liberté en ligne au cours de l'année dernière :

La censure de l'État cible la connectivité mobile. Un nombre croissant de gouvernements a clôturé les services internet mobiles pour des raisons politiques ou de sécurité. La moitié des coupure internet de l'année dernière ont été relatives à la connectivité mobile, et la plupart des autres concernaient les services de téléphonie mobile et fixes. La plupart des coupures mobiles ont eu lieu dans des zones peuplées par des minorités ethniques ou religieuses qui ont défié l'autorité du gouvernement central ou ont cherché à obtenir plus de droits, comme les zones tibétaines de Chine et la région Oromo en Éthiopie. L'accès internet a été coupé, pour des gens déjà marginalisés, qui en dépendent pour la communication, le commerce, et l'éducation.

De plus en plus de gouvernements restreignent les vidéos en direct. Puisque la diffusion de vidéos en direct a gagné en popularité ces deux dernières années, avec l'émergence de plateformes comme Facebook Live et les stories en direct de Snapchat, certains gouvernements ont tenté de restreindre cette tendance, particulièrement durant les protestations politiques, en bloquant les applications de diffusion en direct et arrêtant les gens qui tentent de diffuser des abus. Puisque les journalistes citoyens diffusent en général les protestations politiques sur leurs téléphones, les gouvernements de pays comme la Biélorussie ont déjà perturbé la connectivité mobile

pour empêcher des images en direct d'atteindre de grosses audiences. Les autorités justifient souvent ces restrictions en déclarant que le streaming en live peut être utilisé pour diffuser de la nudité et de la violence, mais les interdictions totales sur ces outils empêchent les citoyens de les utiliser à d'autres fins.

Les attaques technologiques contre des sources d'information, l'opposition, et des défenseurs des droits de l'hommes augmentent. Les cyberattaques deviennent de plus en plus communes, en partie à cause de la disponibilité croissante de technologies appropriées, vendues sur un marché peu réglementé, et en partie à cause de pratiques de sécurité inadéquates chez de nombreux groupes ou individus ciblés. Le coût relativement bas des outils de cyberattaque a permis aux gouvernements centraux mais aussi aux employés gouvernementaux locaux et aux organismes d'application de la loi de les obtenir et de les employer contre leur « ennemis », y compris ceux qui montrent au monde la corruption et les abus. Les blogs indépendants et les sites d'information sont régulièrement mis hors service par des attaques DDoS, les comptes de réseaux sociaux d'activistes sont désactivés et piratés, et les politiciens de l'opposition et les défenseurs des droits de l'homme sont soumis à une surveillance et voient leurs téléphones et leurs ordinateurs illégalement piratés. Dans de nombreux cas, comme au Bahreïn, en Azerbaïdjan, au Mexique, et en Chine, des analystes indépendants ont conclu que c'était le gouvernement qui se trouvait derrière ces attaques.

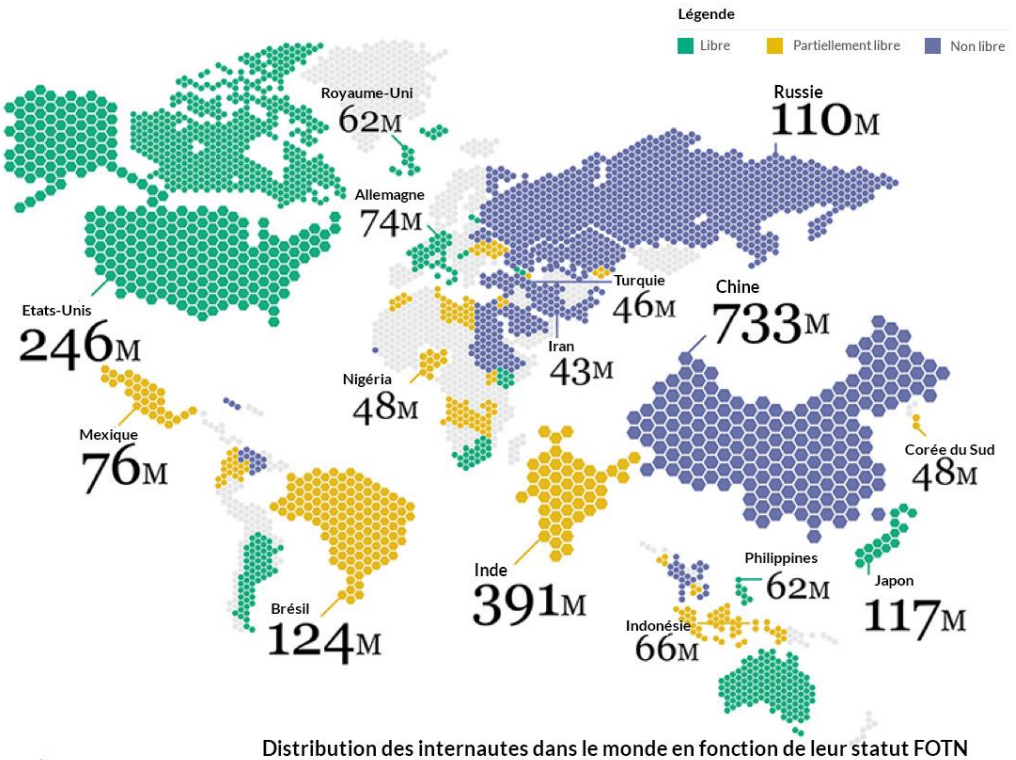
De nouvelles restrictions sur les réseaux virtuels privés (VPN). Bien que les VPN sont utilisés pour de divers usages, y compris par des entreprises qui souhaitent que leurs salariés accèdent aux fichiers de l'entreprise à distance et en toute sécurité, ils sont souvent utilisés dans les régimes autoritaires comme un moyen de contourner la censure internet et accéder à des sites bloqués. Cela fait des VPN une cible pour les censeurs du gouvernement, et 14 pays restreignent actuellement ces connexions d'une manière ou d'une autre, tandis que six pays ont introduit de nouvelles restrictions cette année. Le gouvernement chinois, par exemple, a sorti de nouvelles lois concernant des VPN « approuvés » qui sont probablement plus souples avec les demandes du gouvernement, et a commencé à bloquer certains des services, non approuvés.

Les attaques physiques contre les citoyens du net et les journalistes en ligne ont augmenté drastiquement. Le nombre de pays où des répercussions physiques ont suivi des déclarations en ligne a augmenté de 50 % cette année, entre 20 et 30 pays sur tous ceux analysés. Les cibles les plus fréquentes sont les journalistes et bloggeurs en ligne qui parlent de sujets sensibles, et les individus qui ont critiqué ou se sont moqués des institutions religieuses en place. Dans huit pays, des gens ont été assassinés pour s'être exprimé en ligne. En Jordanie, par exemple, un dessinateur chrétien a été tué par balle après avoir publié un dessin en ligne qui se moquait de la vision du paradis des islamistes, alors qu'à Myanmar, un journaliste d'investigation a été assassiné après avoir posté sur Facebook des notes qui laissaient entendre la présence de corruption.

Bon nombre des pratiques décrites plus haut sont clairement illégales, et marquent une cassure avec les tendances des années précédentes, où les gouvernements se

hâtaient de passer de nouvelles lois qui régulaient l'activité internet et codifiaient les tactiques de censure. Par exemple, répandre de fausses informations et entacher les réputations de certains individus sont des infractions criminelles dans les pays où les gouvernements emploient ce type de tactique contre leurs détracteurs. De la même manière, dans de nombreux pays où le gouvernement semble être à l'origine des cyberattaques qui affectent la communauté des défenseurs des droits de l'homme, des lois récentes sur la cyber sécurité interdisent en réalité de telles pratiques. Même dans le cas des coupures mobiles, la plupart des pays n'ont pas de lois spécifiques autorisant ces perturbations. Il semblerait que dans de nombreux pays, les régulations internet imposées ces dernières années ne s'appliquent en pratique qu'aux citoyens, tandis que les agents gouvernementaux peuvent les ignorer en toute impunité.

Distribution des Internautes dans le monde en fonction du Pays et de leur statut Freedom on the Net (FOTN)



Freedom House
www.freedomonthenet.org

Distribution des internautes dans le monde en fonction de leur statut FOTN

Les 65 pays évalués par Freedom on the Net représentent 87% de la population mondiale d'internautes. Plus de 1,2 milliard d'internautes, ou encore 40% des utilisateurs dans le monde, vivent dans trois pays – la Chine, l'Inde, et les Etats-Unis – qui couvrent l'ensemble du spectre des environnements de la liberté en ligne, de statut de « Libre » à « Non Libre ».

Analyser le déclin mondial

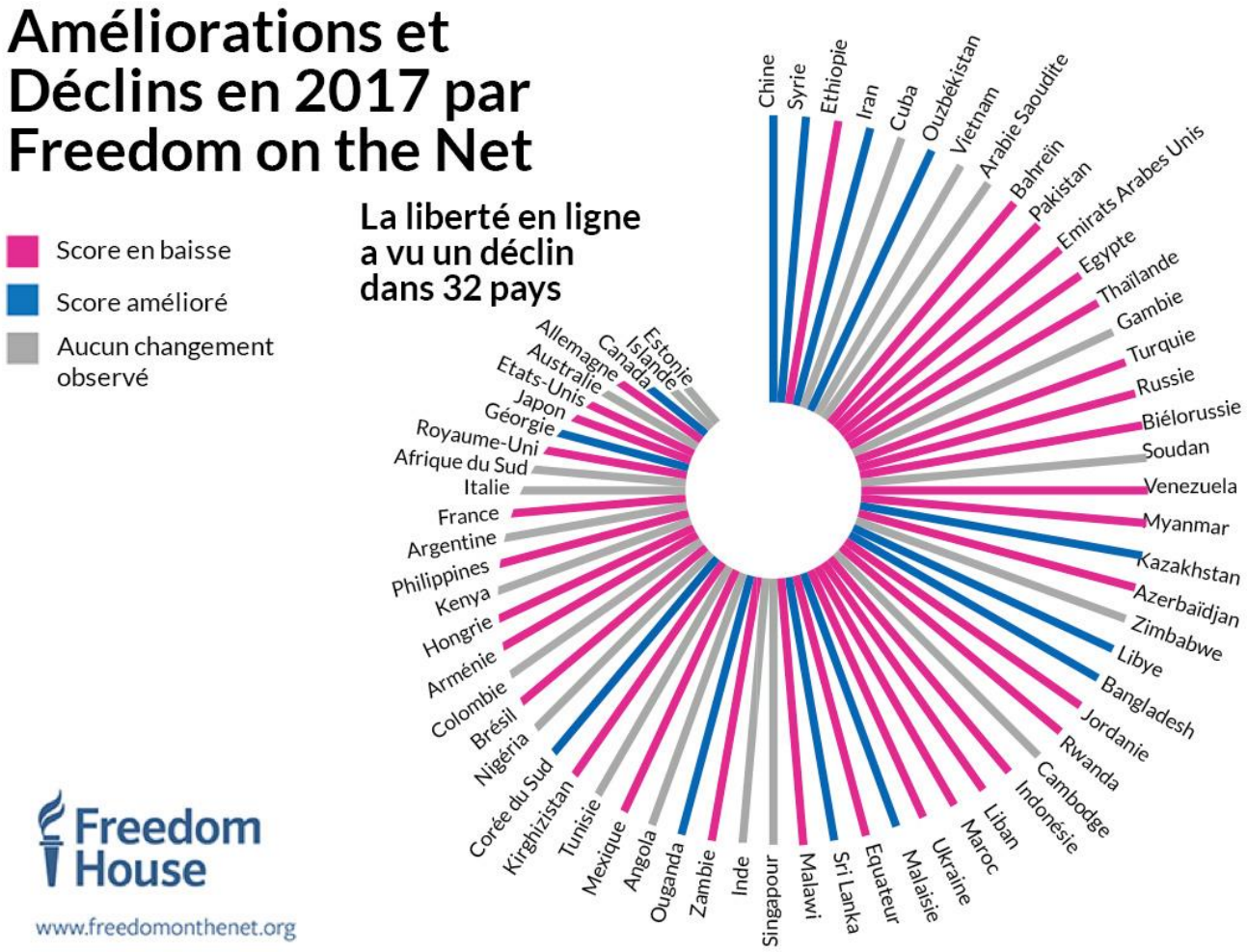
Freedom on the Net est une étude complète sur la liberté du net menée dans 65 pays du globe, et couvrant 87 % des utilisateurs internet du monde. Elle suit chaque année les améliorations et les régressions des politiques et des pratiques gouvernementales.

Les pays inclus dans l'étude sont sélectionnés pour représenter des régions géographiques variées et différents types de régime. Cette étude, la septième du genre, se concentre sur les développements ayant eu lieu entre Juin 2016 et Mai 2017, même si des évènements plus récents ont été inclus dans les rapports individuels de certains pays. Plus de 70 chercheurs, quasiment tous basés dans les pays qu'ils analysent, ont contribué à ce projet en examinant les lois et les pratiques qui concernent internet, en testant la disponibilité de certains sites et services, et en interviewant un large choix de sources.

Sur les 65 pays analysés, 32 subissent une régression générale depuis Juin 2016. Les plus grosses régressions ont eu lieu en Ukraine, en Égypte, et en Turquie. En Ukraine, le gouvernement a bloqué des plateformes russes majeures, y compris le réseau social le plus utilisé du pays (VKontakte) et le plus gros moteur de recherche (Yandex), pour des raisons de sécurité nationale. Les représailles violentes en cas d'activité en ligne ont pris le pays d'assaut, et un journaliste en ligne très connu a été tué dans une attaque à la voiture piégée. En Égypte, les autorités ont bloqué plus de 100 sites web, comme le réseau d'information basé au Qatar, Al-Jazeera, le site d'informations indépendant *Mada Masr*, et la plateforme de blog Medium. Des utilisateurs de réseaux sociaux ont été condamnés à de lourdes peines de prison pour toute une variété de délits douteux, comme par exemple avoir insulté le président du pays. Et en Turquie, des milliers de propriétaires de smartphones ont été arrêté, simplement pour avoir téléchargé l'application de communication cryptée ByLock, qui était disponible de façon publique sur Apple store et Google Play, parmi les accusations on retrouve que l'appli avait été utilisée par les personnes impliquées dans la tentative ratée de coup d'état en Juillet 2016.

C'est la Chine qui a le plus nuit à la liberté du net, pour la troisième année consécutive. Les répressions du gouvernement chinois se sont intensifiées en prévision du 19ème congrès national du Parti Communiste en Octobre 2017, qui accompagnait le deuxième mandat de cinq ans de Xi Jinping en tant que secrétaire général. Les restrictions de cette année incluaient l'ordre officiel de retirer toutes les références en ligne d'une espèce de scarabée fraîchement découverte nommée Xi, nomination que les censeurs ont jugé injurieuse à cause du comportement agressif de l'insecte. Les autorités ont continué à affaiblir la confidentialité des utilisateurs grâce à une nouvelle loi sur la cyber sécurité, qui renforce l'obligation des entreprises internet d'enregistrer les utilisateurs sous leurs vrais noms et d'aider les agences de sécurité avec leurs enquêtes. Les entreprises nationales mettent en place ces mesures de façon progressive dans le but d'avoir un système de "crédit social" – dont le principe est d'assigner des scores numériques aux gens selon leurs modèles d'utilisation d'internet, similaire à un pointage de crédit financier – qui pourrait à long terme rendre l'accès aux services gouvernementaux et financiers dépendant du comportement en ligne des citoyens. La loi sur la cyber sécurité exige également des entreprises étrangères qu'elles stockent les données sur les utilisateurs chinois au sein du pays d'ici 2018, et de nombreuses entreprises ont déjà commencé à s'exécuter, comme Uber, Evernote, LinkedIn, Apple, et AirBnb.

Des détracteurs du gouvernement ont reçu des peines de prison allant jusqu'à 11 ans pour avoir publié des articles dans des sites étrangers. Si de telles sanctions sont documentées année après année, la mort en Juillet 2017 de l'avocat de la démocratie Liu Xiaobo d'un cancer du foie pendant sa détention fut un rappel sombre que l'incarcération a des effets désastreux sur les individus. Liu, gagnant du Prix Nobel de la paix, était en prison depuis qu'un manifeste pro démocratie qu'il avait co-écrit avait été publié en ligne en 2009. L'annonce de sa mort a déclenché une vague de soutien – et de censure.



La liberté du net au Venezuela et en Arménie a régressé. Le Venezuela est passé de statut de Partiellement libre à Non libre à cause de mesures répressives de plus en plus fortes contre les droits politiques et les libertés civiles suite à la déclaration du Président Nicolás Maduro en Mai 2016 de « l'état d'urgence économique exceptionnel » renouvelé en Mai 2017. Le gouvernement a bloqué quelques sites qui proposaient une couverture en direct des manifestations contre le gouvernement en proclamant que ces sites « incitaient à la guerre ». Des gangs armés ont physiquement attaqué des

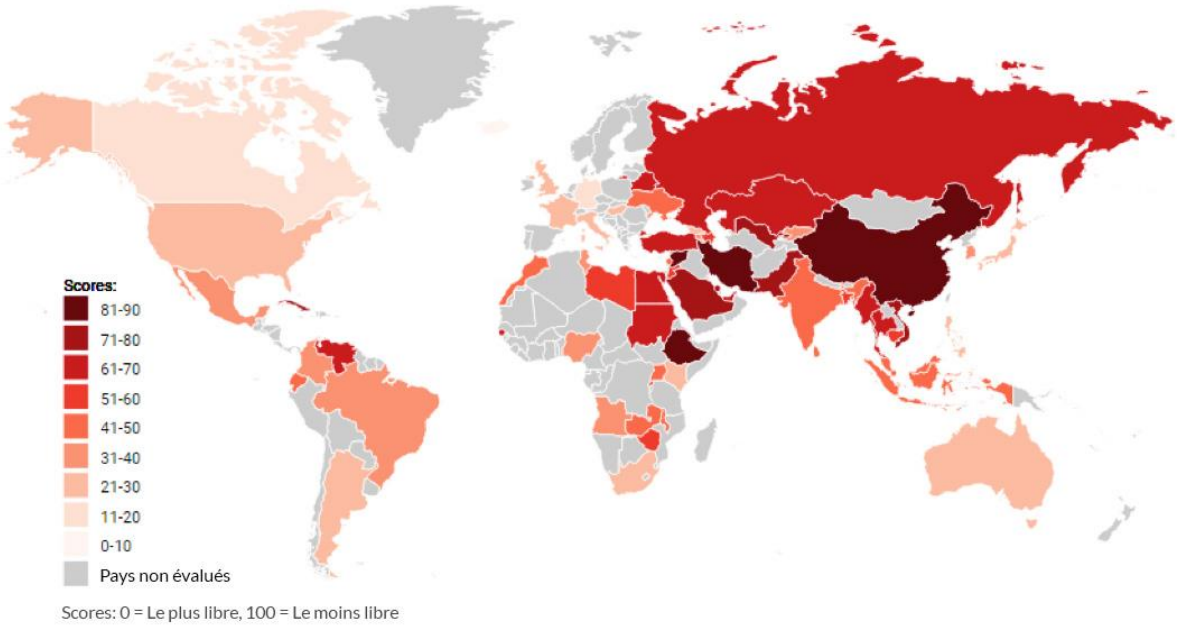
citoyens et journalistes en ligne qui tentaient de filmer les manifestations, tandis que l'opposition subissait une vague sans précédent de cyber attaques, qui provoquaient le blocage répétitif de leurs sites pour une durée indéterminée, ainsi que la désactivation de leurs comptes. En Arménie, pays qui est passé de Libre à Partiellement libre, la police a attaqué et empêché des journalistes et citoyens du net de diffuser en direct des manifestations antigouvernementales. Des milliers de personnes ont protesté en réponse à la mauvaise gestion de la police d'une situation de prise d'otages, pendant laquelle des employés gouvernementaux ont temporairement restreint l'accès à Facebook.

Les États-Unis ont également subi un déclin de la liberté sur le net. Si l'environnement en ligne aux États-Unis reste dynamique et varié, la prépondérance de contenus de désinformation provenant de partisans extrémistes a eu un impact significatif. La prolifération de « fake news » ou intox, surtout sur les réseaux sociaux, a atteint des sommets durant la période précédant les élections présidentielles de Novembre 2016, mais elle continue à inquiéter. Des journalistes remettant en question les positions de Donald Trump ont subi du harcèlement en ligne poussé.

Parmi d'autres développements notables, après que Trump ait endossé le rôle de président en Janvier 2017, l'agence américaine de douane et de protection des frontières a exigé de Twitter qu'il révèle le nom du propriétaire d'un compte qui s'opposait à la politique d'immigration de Trump, et n'a retiré sa demande qu'après que l'entreprise ait fait appel aux tribunaux. Encore plus inquiétant, le gouvernement a demandé à l'entreprise d'hébergement DreamHost en Juillet 2017 de divulguer toutes les adresses IP des utilisateurs ayant visité disruptj20.org, un site qui a aidé à coordonner les manifestations durant l'investiture de Trump ; cette requête a été annulée après que DreamHost ait saisi la justice. Pendant ce temps, le président de la Commission Fédérale des Communications a annoncé en Avril un plan pour faire régresser les mesures de protection de la neutralité du net adoptées en 2015.

Seulement 13 pays ont vu une amélioration de leur score de liberté du net. Dans la plupart des cas, les gains étaient limités et ne reflétaient pas de changements de caps plus importants. En Libye, par exemple, plusieurs sites d'informations ont été débloqués, et contrairement aux années précédentes, aucun utilisateur n'a été mis en prison pour ses activités en ligne. Au Bangladesh, il n'y a pas eu de réitération des blocages temporaires des applis populaires telles que Facebook, WhatsApp, et Viber qui avaient eu lieu en 2015, malgré des inquiétudes quant à la sécurité suite à la confirmation de sentences de peine de mort contre deux leaders islamistes. Finalement l'Ouzbékistan, l'un des pays les plus restrictifs de cette étude, a connu une légère amélioration après l'introduction d'une nouvelle plateforme gouvernementale en ligne, conçue pour traiter les demandes publiques, incitant un meilleur engagement des citoyens.

Scores globaux 2017 par Freedom on the Net



Scores: 0 = Le plus libre, 100 = Le moins libre

Développements majeurs

Les bots et l'intox ajoutent de la sophistication à la manipulation en ligne

Les régimes répressifs cherchent depuis longtemps à contrôler le flux d'informations au sein de leurs territoires, une tâche rendue plus difficile depuis l'avènement d'internet. Quand les lois punitives, la censure en ligne et d'autres tactiques répressives se montrent peu adaptées et inefficaces, de plus en plus de gouvernements produisent leur propre contenu pour modeler le paysage numérique en leur faveur. Freedom House a commencé à pister l'utilisation de commentateurs rémunérés et pro gouvernement en 2009, mais de plus en plus de gouvernements emploient désormais toute une gamme de tactiques de manipulation sophistiquées qui bien souvent servent à se renforcer entre elles. Les autoritaristes se sont saisi des mêmes outils que ceux utilisés par de nombreux activistes démocratiques pour perturber la version officielle des médias de l'état, et les ont détourné pour en faire une arme antidémocratique.

La tentative du gouvernement russe d'utiliser des bots et de l'intox pour influencer les élections aux États-Unis et en Europe de l'ouest a attiré une attention nouvelle sur le problème de la manipulation de contenu. Cependant dans de nombreux pays, ces tactiques ne sont pas utilisées par des puissances étrangères, mais par les gouvernements en place et les partis politiques cherchant à préserver leur emprise.

Des commentateurs pro gouvernement prétendent avoir le soutien populaire

Des commentateurs pro gouvernement sont présents dans 30 des 65 pays analysés dans cette étude, dont 23 déjà présents dans l'édition 2016, et c'est un nouveau record. Dans ces pays, des rapports fiables ont établi que le gouvernement emploie du personnel ou paye des contractuels pour manipuler les discussions en ligne sans que la nature sponsorisée du contenu ne soit explicite. Les preuves ont été rassemblées grâce à du journalisme d'investigation, à des documents gouvernementaux qui ont fuité et grâce à de la recherche académique. La manipulation a trois objectifs principaux : (1) feindre le soutien populaire pour le gouvernement (ce qu'on appelle aussi "astroturfing"), (2) salir les opposants du gouvernement, et (3) détourner les conversations en ligne de sujets controversés. Les commentateurs pro gouvernement ont eu pour tâche de s'occuper de ces objectifs de diverses manières.

Dans les pays les plus répressifs, des bureaucrates gouvernementaux et des représentants de la sécurité sont directement employés pour manipuler toute discussion politique. Par exemple, les « cyber djihadistes » du Soudan, une unité du Service national de renseignement et de la sécurité ont créé de faux comptes pour infiltrer des groupes populaires sur Facebook et WhatsApp, créer un soutien pour les politiques gouvernementales, et dénoncer les journalistes critiques. Un des responsables de la propagande au Vietnam a admis avoir géré une équipe d'une centaine de « faiseurs d'opinion publique » qui surveillaient et dirigeaient les discussions sur tout, de la politique étrangère aux droits fonciers.

Dans d'autres cas, la manipulation en ligne est confiée aux équipes du parti dirigeant, ses consultants politiques et ses entreprises de relations publiques. Des reportages et investigations ont montré le rôle de l'Internet Research Agency, une « ferme à trolls » russe apparemment financée par un homme d'affaire proche du président Vladimir Poutine. Aux Philippines, d'anciens membres d'une « armée du clavier » ont affirmé gagner 10 $ par jour pour gérer de faux comptes de réseaux sociaux qui soutenaient Rodrigo Duterte ou attaquaient ses détracteurs durant la période précédant son élection en Mai 2016, et bon nombre d'entre eux sont restés actifs sous son administration, donnant l'impression d'un soutien unanime lors de ses répressions brutales contre des trafiquants de drogue. En Turquie, de nombreuses sources citent une organisation du nom de "AK Troller," ou " Trolls blancs," appelés ainsi en honneur au parti de la Justice et de Développement, dont l'acronyme turque AK signifie également "blanc" ou "propre." Environ 6000 personnes auraient été engagées par le parti pour manipuler des discussions, mettre en place certains agendas, et contrer les opposants du gouvernement sur les réseaux sociaux. Des journalistes et chercheurs, critiques du gouvernement, ont dû faire face à un harcèlement organisé sur Twitter, par des dizaines voire des centaines d'utilisateurs.

Au fil des ans, les gouvernements ont trouvé de nouvelles méthodes pour déléguer la manipulation à des citoyens afin d'obtenir un impact plus grand et éviter de devoir en assumer les responsabilités directes. Le résultat est qu'il peut être compliqué de discerner la propagande du véritable nationalisme populaire, même pour des observateurs avertis. Par exemple, le gouvernement chinois emploie depuis longtemps du personnel d'état pour manipuler les conversations en ligne, mais ils font désormais partie d'un écosystème bien plus gros, qui compte des volontaires du parti dirigeant mais aussi des citoyens ordinaires, qu'on appelle des "ziganwu." Sur les documents officiels, la Communist Youth League a décrit ces « volontaires du net » comme des gens utilisant leur « clavier comme arme » pour défendre leur « mère patrie » dans la « guerre du net » en cours.

Dans au moins 8 pays, des politiciens encouragent ou même incitent leurs partisans à signaler les « contenus anti patriotiques », harceler « les ennemis de l'État » ou inonder les réseaux sociaux de commentaires louant les politiques du gouvernement, travaillant souvent main dans la main avec des commentateurs payés, et des représentants de la propagande. Un membre de la police en Thaïlande a invité les citoyens à être les yeux et les oreilles de l'État après le coup d'état militaire de 2014, offrant 15 $ à ceux qui signalaient des utilisateurs qui s'opposaient au gouvernement militaire. De plus, plus de 100 000 étudiants ont été formés comme « cyber scouts » pour surveiller et signaler les comportements en ligne qui peuvent nuire à la sécurité nationale, tandis que les supporters du régime lancent de véritables chasses aux sorcières sur Facebook, identifiant et signalant les utilisateurs qui ne respectent pas les lois strictes contre la critique de la monarchie. En Équateur, l'ancien président Rafael Correa a lancé un site web qui envoyait une notification à ses partisans à chaque fois qu'un utilisateur de réseau social critiquait le gouvernement, permettant ainsi à tous les commentateurs pro gouvernement de cibler les dissidents politiques.

Les Bots noient les activistes sous un torrent d'absurdités et de discours haineux

En plus des commentateurs humains, on constate une augmentation des comptes automatisés sur les réseaux sociaux afin de manipuler les discussions en ligne. Dans au moins 20 pays, des comportements d'activité en ligne caractéristiques suggèrent l'utilisation de tels "bots" pour influencer le discours politique. Des milliers de faux profils et faux noms peuvent être déployés en un clic, programmés avec des algorithmes pour viser certains médias ou mots clés. Ils parviennent à noyer la dissidence et les tentatives de lancement d'action collective en ligne.

Selon les estimations du fournisseur de services sur cloud Imperva Incapsula, les bots représentaient jusqu'à 51,2 % du trafic web en 2016. Bon nombre d'entre eux effectuent des tâches automatisées dans un but commercial. Par exemple, les bots jouent

désormais un rôle vital dans la surveillance de l'état de sites web, la commande de produits en ligne, et pour permettre la diffusion de nouveau contenu des sites vers les applications mobiles. Ces « bon bots » se reconnaissent, et sont gérés par de nombreuses grosses entreprises, comme Amazon, Facebook, Google, et Microsoft. Les bots malicieux, toutefois, sont conçus pour être inidentifiables et représentent la majorité des activités de bots depuis 2013. On peut s'en servir pour pirater, spammer, voler des contenus et les faire passer pour des humains dans des discussions publiques.

Des études ont prouvé la difficulté de détecter ces bots avec un seul critère. Sur Twitter, les comptes bots tweetent en général plus fréquemment, se retweetent entre eux, et renvoient plus souvent vers des liens externes, en comparaison aux comptes gérés par des humains. Les bots sont également utilisés pour obtenir des « likes » et des abonnés artificiels. Par exemple, une analyse des abonnés twitter du Président Donald Trump faite par *Newsweek* en Mai a déterminé que seulement 51 pourcent de ses 30 millions d'abonnés étaient réels.

Dans certains cas, des bots malicieux ont été déployés dans des guerres de l'information menées par des gouvernements, contre leurs adversaires étrangers et leur opposants domestiques.

Au Mexique, environ 75 000 comptes automatisés appelés les Peñabots ont été utilisés pour submerger l'opposition politique sur Twitter. Quand un nouvel hashtag émerge pour parler d'une manifestation ou d'une histoire de corruption, le gouvernement emploie deux méthodes pour orienter le système en faveur du président Enrique Peña Nieto. Pour ce qui est de la première méthode, les bots mettent en avant d'autres hashtags afin de faire disparaître les hashtags problématiques du top 10. En ce qui concerne la seconde, appelée le « hashtag empoisonné », les bots inondent les hashtags antigouvernementaux avec des publications non pertinentes pour enterrer toute information. Cette seconde méthode peut avoir de véritables conséquences : incapables d'accéder aux cartes indiquant les activités de la police et les routes de sorties sûres, de nombreux manifestants pacifiques du Mexique n'ont pas pu quitter les zones de danger et ont subi des représailles excessives de la part de la police.

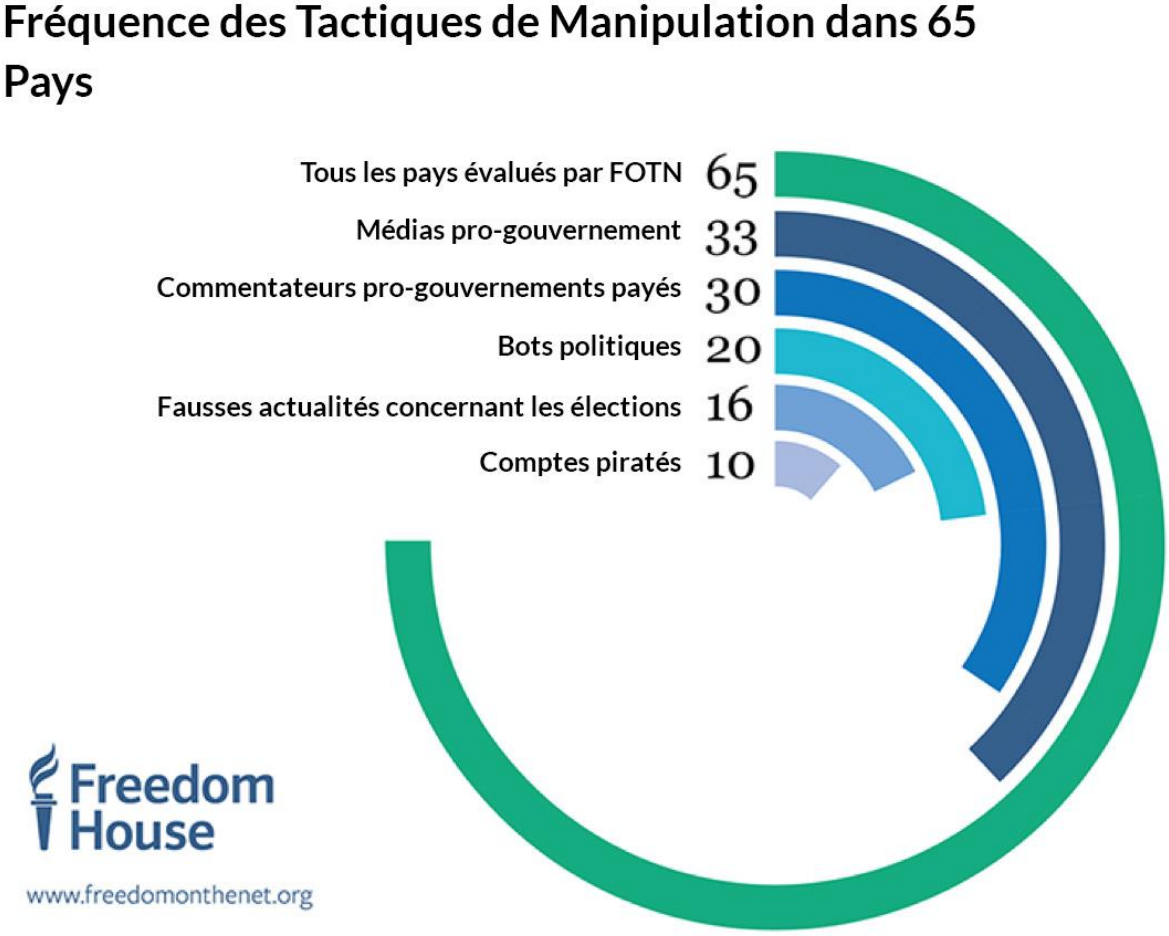
Les bots peuvent aussi être utilisés pour salir les opposants du régime et promouvoir le sectarisme. Au Bahreïn, par exemple, où une grosse partie de la majorité Chiite a exigé une réforme politique de la monarchie Sunnite répressive, un chercheur a découvert que plus de la moitié des tweets avec l'hashtag #Bahreïn sur une certaine période de temps étaient des tweets haineux anti-Chiite. Des tweets, avec un langage quasiment identique, ont accusé un clerc Chiite d'incitation à la violence contre les forces de l'ordre. Cette armée de bots a été mobilisée dans des conversations en ligne à propos de l'Arabie Saoudite, du Yémen, et de l'Iran, à chaque fois pour dénigrer les musulmans Chiites.

Des comptes piratés répandent la désinformation

Dans au moins 9 pays, des hackers qu'on suspecte être liés au gouvernement ou au parti dirigeant ont piraté des comptes de réseaux sociaux et des sites d'informations pour répandre la désinformation. Au Moyen-Orient, le piratage présumé d'un site d'informations Qatari permettant le partage de publications pro-iraniennes attribuées à des fonctionnaires Qataris hauts placés a créé un incident international. Si le Qatar nie la véracité de cette histoire, une coalition régionales menée par l'Arabie Saoudite a répondu par un blocage d'une douzaine de sites d'information Qataris. Pendant l'hystérie que cela a engendré, les autorités égyptiennes ont également bloqué l'accès à des dizaines de sites d'informations indépendants et à des sites de plusieurs organisations pour les droits de l'homme.

Si les allégations de piratage contre le Qatar doivent encore être confirmées de manière indépendante, ce ne serait pas un cas isolé. La veille des manifestations du « Jour de la liberté » en Biélorussie, le compte Facebook d'un leader de l'opposition et organisateur de manifestation a été piraté afin de publier de faux commentaires dissuadant les gens de participer à cette manifestation. En Turquie, des hackers ont pris le contrôle de comptes de journalistes et activistes proéminents le tout dans le but de publier de fausses excuses dans lesquelles les victimes expriment leur regret d'avoir critiqué le gouvernement. Access Now a déclaré qu'au Venezuela, à Myanmar, et au Bahreïn, des hackers répandent la désinformation avec des attaques « DoubleSwitch ». Après avoir réussi à accéder à un compte vérifié, ils changent l'adresse de récupération et altèrent le pseudonyme puis créent un nouveau compte avec le pseudonyme original de la victime, et publient des contenus depuis les deux comptes.

Ces incidents soulignent le rôle d'une cybersécurité faible concernant la manipulation en ligne. De nombreux hackeurs exploitent les faiblesses des systèmes d'authentification par SMS à deux facteurs des réseaux sociaux, surtout si la victime réside dans un pays où des hackeurs sponsorisés par l'État peuvent travailler de concert avec des compagnies de télécommunication nationales. Les entreprises internationales de technologie ont fait des efforts dans la surveillance des attaques sponsorisées par l'État, mais le vol répété des données clients et les fuites exploitées par les cybers criminels peuvent fournir assez d'informations aux hackeurs pour contourner les obstacles de l'identification.



De fausses informations prolifèrent dans un nouvel environnement médiatique

La « démocratisation » de la production de contenu et la centralisation des chaînes de distribution en ligne comme Twitter et Facebook ont secoué l'industrie des médias, et ont eu pour conséquence imprévue de donner naissance à une prolifération d'intox, c'est-à-dire de fausses informations données intentionnellement et créées pour ressembler à de véritables nouvelles et générer un maximum d'attention. L'intox existe depuis les débuts de la presse écrite. Toutefois, ses utilisateurs ont récemment développé de nouvelles façons sophistiquées, comme de jouer avec les algorithmes des réseaux sociaux et des moteurs de recherche, pour atteindre des audiences plus larges et tromper les nouveaux utilisateurs.

Les réseaux sociaux sont de plus en plus utilisés en tant que source primaire d'informations, mais l'incapacité des utilisateurs à distinguer les vraies informations des fausses leur fait perdre de la valeur et de l'utilité. S'il n'y a que peu d'informations publiquement disponibles en ce qui concerne les algorithmes de Facebook, Google, Twitter, ils ont tendance à promouvoir des articles viraux ou provocants qui génèrent des clics, peu importe la véracité du contenu. De même la même façon que des organisations médiatiques arrivistes telles que BuzzFeed adaptent les titres de vrais articles afin de convenir au fil d'actualité de Facebook ; des adolescents macédoniens ont créé des titres accrocheurs pour de faux articles avant les élections américaines de Novembre 2016, profitant des Google Ads placées sur leurs sites. Ces contenus illégaux et faux apparaissaient sur les réseaux sociaux juste à côté d'articles sérieux, avec aucun moyen de différencier facilement entre les deux.

Freedom House a documenté des exemples frappants de fausses informations autour des périodes d'élections et de référendums dans au moins 16 des 65 pays analysés. Des agents gouvernementaux du Venezuela ont régulièrement fait appel à des images manipulées pour disséminer des mensonges sur les partisans de l'opposition sur les réseaux sociaux, créant une confusion immense et anéantissant la crédibilité des opposants juste avant les élections. Au Kenya, des utilisateurs ont partagé des articles et vidéos d'intox qui portaient les logos de médias dignes de confiance comme CNN, BBC, et NTV Kenya sur les réseaux sociaux et les applis de messagerie avant les élections d'août 2017.

Si les sites d'intox n'ont rien de nouveau, ils sont désormais de plus en plus utilisés avec sophistication pour des raisons politiques. Des acteurs pro gouvernement iraniens ont créé depuis longtemps des sites comme persianbbc.ir qui ressemblent au vrai bbcpersian.com, afin de les remplir de théories du complot et de propagande anti occidentale. Plus récemment, des groupes de hackeurs iraniens ont établi des sites web avec des noms comme BritishNews et AssadCrimes pour mieux apparaitre sur les moteurs de recherche. Ce dernier contenait des articles récupérés sur un blog de l'opposition syrienne et fut faussement enregistré sous le nom d'un activiste de l'opposition connu. Les hackeurs ont créé des adresses email et des profils de réseaux sociaux reliés à ces fausses publications afin de communiquer avec les opposants du gouvernement et les défenseurs des droits de l'homme pour analyser leur réseau social. Une fois la confiance établie, les hackeurs ciblaient les victimes avec des programmes d'accès à distance par cheval de Troie (RAT) et obtenaient l'accès à leurs appareils.

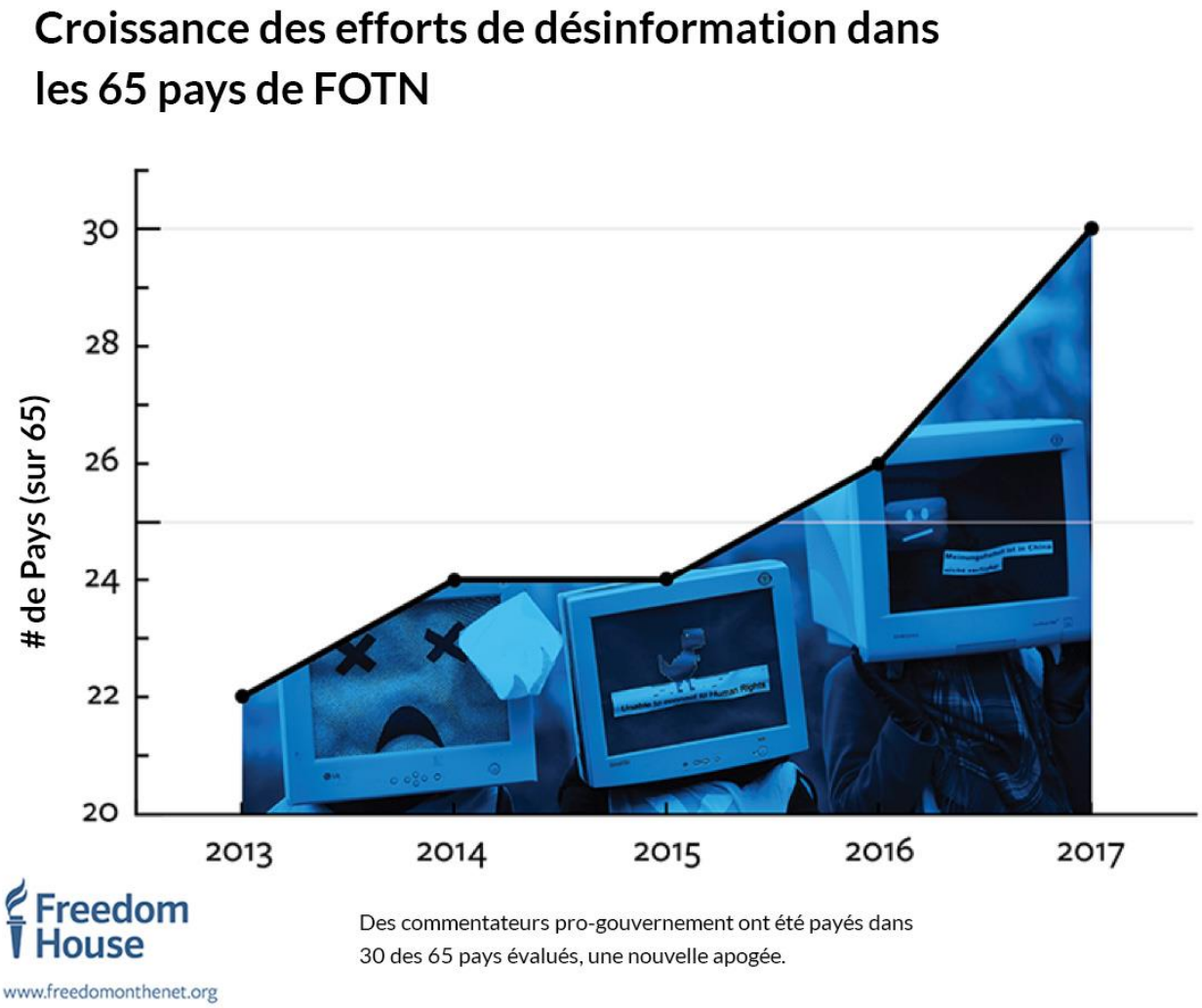
Nouvelles « pro gouvernement » et propagande

La ligne entre véritables informations et propagande est souvent difficile à discerner, surtout dans des environnements extrêmement partisans où les deux côtés s'accusent

mutuellement de détourner les faits. Les sociétés qui ont un respect poussé pour la liberté de la presse et de parole permettent aux citoyens de consulter une gamme variée d'informations et de sources afin de se faire une idée des évènements. Toutefois, dans plus de la moitié des pays inclus dans le rapport, le paysage médiatique en ligne est perturbé par la corruption, les directives éditoriales politisées, ou les prises de contrôle par des entités et des personnes affiliées au gouvernement, ce que Freedom House observe depuis des années dans les secteurs de la presse et de la diffusion. Le résultat, c'est bien souvent un environnement dans lequel tous les plus gros médias jouent selon les règles gouvernementales.

En Azerbaïdjan, le pluralisme des médias a souvent été entaché par des restrictions sur les financements étrangers qui forcent les médias à dépendre du marché publicitaire local contrôlé par l'état. En Hongrie et en Russie, le gouvernement ou les oligarques avec des liens avec le parti dirigeant ont acheté de nombreux sites d'information, viré leurs journalistes critiques, et rapidement changé le point de vue éditorial du site. Certains des plus fervents acteurs de la propagande d'état sont des gouvernements prétendant combattre la désinformation. À Cuba, où des lois ont rendu criminelle la diffusion de « propagande ennemie » et « d'informations non autorisées », les médias en ligne sont depuis longtemps dominés par des médias tenus par le gouvernement et des bloggeurs pro gouvernement qui défendent les actions des dirigeants et de leurs alliés étrangers. La constitution interdit de posséder un média, et n'autorise la liberté de parole et la liberté de la presse seulement si elle est « conforme aux objectifs d'une société socialiste ».

Mais il existe peu d'endroits où le rapport entre propagande d'état et restrictions légales sur les médias est aussi hypocrite qu'en Russie. Les bloggeurs avec plus de 3000 visiteurs quotidiens doivent donner leurs informations personnelles au gouvernement russe et respecter les lois de régulation des médias de masse. Les moteurs de recherches et les agrégateurs d'informations se sont vus interdire la publication d'histoires provenant de sources non validées, par une loi qui a pris effet en Janvier 2017. Les plateformes de réseaux sociaux étrangers ont dû déplacer leurs serveurs au sein du pays pour en faciliter le contrôle par l'état, pendant que les plateformes locales majeures se faisaient racheter par des amis du Kremlin.



Diverses réponses à la manipulation

Dans une tendance inquiétante, les gouvernements d'au moins 14 pays ont restreint la liberté du net, dans une tentative de gestion des nombreuses formes de manipulation de contenus. En Ukraine, l'un des premiers pays à subir la guerre de l'information moderne russe, des agents russes ont créé des faux sites d'informations ukrainiens et ont inondé les réseaux sociaux avec des rapports fabriqués de toutes pièces qui faisaient part du désir de la Crimée de rejoindre la Russie, du rejet de l'Union Européenne par les citoyens ukrainiens, et d'autres histoires qui promeuvent l'agenda russe. En réponse, les autorités ukrainiennes ont bloqué de nombreuses plateformes de réseaux sociaux et de nombreux moteurs de recherche russes, rejoignant la liste des pays qui ont banni les gros réseaux sociaux, comme la Chine et l'Iran. Les sites touchés, comme Odnoklassniki, VKontakte, Yandex, et Mail.ru, étaient très utilisés par les ukrainiens.

De nombreux pays démocratiques se penchent sur le problème des fausses informations et de façon plus générale, sur la responsabilité qu'ont les intermédiaires, comme Google, Facebook, et Twitter, de retirer les contenus frauduleux ou illégaux. La loi sur les réseaux sociaux d'Allemagne votée en Juin 2017, oblige les entreprises à retirer les contenus étiquetés comme illégaux dans un processus qui manque de surveillance judiciaire. Cette loi est profondément problématique et peut inciter les entreprises de réseaux sociaux à effacer rapidement tous les contenus controversés, même s'il s'agit de simple liberté d'expression, pour éviter des amendes allant jusqu'à 50 millions d'euros. Avec des projets similaires en Italie et aux Philippines, la loi allemande peut créer un précédent pour les gouvernements, qu'ils soient démocratiques ou répressifs, sur les manières d'utiliser des pressions légales pour s'assurer que les entreprises se conforment aux demandes locales de censure. D'une façon plus générale, il faudra un temps considérable, des ressources et de la créativité pour réussir à combattre la manipulation de contenus et restaurer la confiance en les réseaux sociaux d'une manière qui n'affaiblit pas la liberté du net et de la presse. Une prise de conscience publique a poussé les entreprises internet à redoubler d'efforts pour supprimer les comptes automatisés et signaler les fausses informations. Plus de 30 000 faux comptes ont été supprimés de Facebook avant les élections françaises de 2017, et Google a modifié ses résultats de recherche pour privilégier les sources d'informations fiables. Twitter a également annoncé sa volonté d'en faire plus pour détecter et suspendre les comptes utilisés dans le seul but de manipuler la discussion sur des sujets clés.

Mais les plateformes de réseaux sociaux et les moteurs de recherche ne sont qu'une partie du puzzle. Des organisations comme First Draft News et Bellingcat offrent aux journalistes, professionnels ou amateurs, les outils nécessaires pour vérifier l'origine des contenus, surveiller les campagnes de manipulation, et afin de prouver la nature erronée des fausses infos. Il faut en faire plus et offrir des solutions locales et sur mesure au problème de manipulation dans différents pays. C'est tout particulièrement le cas quand les gens reçoivent leurs infos sur des plateformes de messagerie instantanée comme WhatsApp et Telegram, où il est encore plus dur de détecter les fausses informations.

Les censeurs de l'Etat visent la connectivité mobile

Les coupures de réseau – définies par Freedom House comme des restrictions intentionnelles de la connectivité des réseaux internet fixes, des réseaux mobiles ou des deux – ont eu lieu dans un nombre de pays croissant ces dernières années. Dans l'édition 2017, 19 pays sur 65 ont subi au moins une coupure de réseau pendant la durée de l'analyse, contre 13 pays dans l'édition 2016 et 7 dans celle de 2015. L'année passée, les autorités ont souvent invoqué la sécurité nationale et publique pour fermer les réseaux de communication, mais les véritables raisons allaient de conflits armés et

malaise social à manifestations paisibles, élections, et rumeurs en ligne pouvant causer des remous.

Les autorités visent de plus en plus les services mobiles plutôt que les réseaux internet fixes. Pendant la période de couverture de cette étude, des perturbations sur mobile uniquement ont été signalées dans 9 des 19 pays où des coupures ont été enregistrées, tandis que les incidents dans le reste des pays touchaient simultanément les lignes fixes et mobiles. Des coupures ciblant les réseaux internet fixes n'ont été signalées que dans deux pays, et furent attribuées aux autorités qui testaient leur capacité à imposer des coupures plus larges à l'avenir.

Il existe plusieurs raisons pour lesquelles les gouvernements visent tout particulièrement la connectivité mobile. D'abord, l'internet mobile est devenu la méthode d'accès la plus répandue dans le monde, avec un trafic mobile mondial qui a surpassé les réseaux fixes pour la première fois fin 2016. Dans de nombreux pays en voie de développement, la majorité des utilisateurs d'internet accède au web avec des appareils mobiles grâce aux prix de plus en plus abordables des abonnements et des appareils, comparé aux abonnements à des réseaux fixes. De plus, les réseaux fixes et les connexions Wi-Fi sont liées à des endroits ou infrastructures spécifiques, tandis que les connexions mobiles permettent aux utilisateurs de se connecter dès qu'ils ont du réseau, ce qui rend les coupures très efficaces.

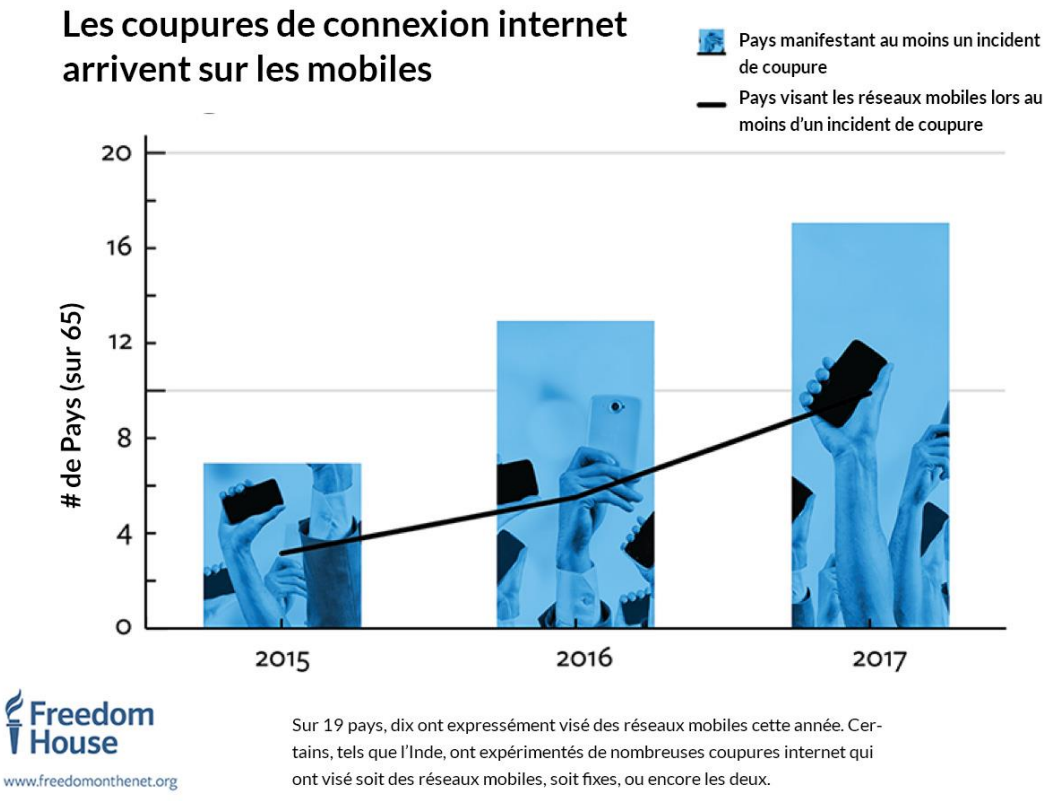
Les réseaux mobiles sont aussi ciblées à cause de la facilité avec laquelle les gens peuvent communiquer et s'organiser en temps réel avec des appareils mobiles, fonctionnalité utilisée à la fois par les manifestants pacifiques et les violents terroristes. Les coupures de réseau mobile permettent aussi de préserver les réseaux fixes pour que les entreprises et les institutions gouvernementales puissent accéder à internet, ce qui peut aider à réduire l'impact négatif de telles restrictions sur l'économie.

Les coupures mobiles isolent les communautés marginalisées

Dans une nouvelle tendance inquiétante, les autorités d'au moins 10 pays ont volontairement perturbé la connectivité mobile de certaines régions, ciblant souvent des ethnies ou groupes religieux persécutés. En Chine, par exemple, les communautés tibétaines et Uigurs ont fait face à des coupures de connectivité mobiles régulières pendant des années, plus récemment dans une zone tibétaine de la province de Sichuan où le gouvernement a tenté d'empêcher que les nouvelles d'un moine tibétain, qui s'était immolé en protestation contre la répression du gouvernement, ne se répandent. En Éthiopie, le gouvernement a coupé les réseaux mobiles pendant presque deux mois dans le cadre d'un état d'urgence décrété en Octobre 2016 suivant les manifestations à grande échelle des populations Oromo and Amhara privées de leurs droits.

Pour beaucoup de communautés affectées par des coupures si localisées, les réseaux mobiles sont la seule option, que ce soit pour le prix ou la disponibilité à cause d'infrastructures fixes sous-développées dans les régions isolées. En conséquence, les coupures peuvent réduire au silence une communauté spécifique, en les empêchant d'attirer l'attention sur leurs griefs politiques et sociaux, mais également en diminuant leurs opportunités économiques et éducatives.

En plus de leur croissante fréquence, les coupures des dernières années ont duré plus longtemps, avec au moins trois pays, le Liban, Bahreïn, et le Pakistan ayant fait l'expérience de coupures régionales de plus d'un an. Au Liban, 160 000 résidents de la ville frontière d'Arsal au nord-est, des réfugiés syriens pour la plupart, ont vu les services d'internet mobile inaccessibles pendant plus de deux ans, comme mesure de sécurité pendant les affrontements fréquents entre les militaires et les militants extrémistes. Depuis juin 2016, les autorités du Bahreïn exigent des compagnies de télécom qu'elles désactivent les connexions fixes et mobiles durant les couvre-feux nocturnes de la ville de Duraz, où des sympathisants d'un clerc Chiite populaire manifestaient contre les persécutions de la monarchie Sunnite.



Les coupures coïncident avec des élections et des événements spéciaux

Les coupures mobiles ont également été utilisées pour freiner les groupes d'opposition pendant des périodes d'élections controversées. Durant les élections présidentielles de la Zambie en août 2016, les réseaux mobiles ont été perturbés pendant 72 h dans des régions dominées par l'opposition à la suite de manifestations de supporters de l'opposition qui ont accusé la commission électorale de fraude. De la même façon, en Gambie, les réseaux furent coupés la veille de l'élection présidentielle de Décembre 2016, mais victoire surprise pour la démocratie, puisque cette tactique n'a pas suffi à faire réélire l'autoritariste Yahya Jammeh, président depuis 22 ans.

Certains gouvernements ont restreint les communications mobiles pendant de gros évènements, de peur qu'ils soient utilisés contre la sécurité publique. L'année passée, les autorités d'au moins trois villes des Philippines ont demandé aux fournisseurs de service de fermer les réseaux mobiles pendant des festivals et parades publics ; et avaient précédemment restreint ce genre de service durant une visite du pape en 2015. Si les coupures étaient courtes, avaient une faible portée et avaient été communiquées au public, ces évènements répétés ont permis de normaliser de telles coupures et de les faire passer comme des mesures gouvernementales légitimes, malgré leur nature disproportionnée et leur effet profond sur la liberté d'expression.

Les restrictions d'applis et les augmentations de prix freinent l'accès au mobile

Les méthodes indirectes de contrôle de la connectivité mobile reçoivent moins d'attention que les coupures, mais elles peuvent avoir le même effet sur la perturbation de communications essentielles. Restant dans la tendance déjà constatée dans *La liberté du Net 2016*, des applis mobiles très populaires ont été fréquemment prises pour cibles ces dernières années. WhatsApp reste l'outil de communication le plus visé, avec des perturbations recensées dans 12 des 65 pays analysés. En Turquie, par exemple, les autorités ont régulièrement entravé le trafic WhatsApp pour le rendre quasiment inaccessible durant des évènements politiques importants. De même le gouvernement du Zimbabwe l'a bloquée pendant plusieurs heures lors de grosses manifestations anti gouvernement.

De fausses régulations des prix de forfait internet sur mobile ont également été utilisées pour restreindre indirectement l'accès à internet. Après le déblocage de WhatsApp au Zimbabwe, le gouvernement a fait augmenter le prix des données mobiles de 500 % pour limiter l'organisation civile. Bien que les réseaux mobiles ne soient pas complètement coupés dans l'état difficile du Jammu-et-Cachemire en Inde, les autorités suspendent fréquemment les forfaits de données internet prépayés, ce qui affecte plus

fortement les résidents à faibles revenus qui ne peuvent pas se permettre de payer un abonnement.

Les gouvernements restreignent les vidéos en direct, surtout pendant les manifestations

Des utilisateurs internet ont fait face à des restrictions ou des attaques pour avoir diffusé des vidéos en live dans au moins 9 pays. Les outils et chaînes de diffusion en direct furent sujet à des blocages, et plusieurs personnes furent placées en détention afin de stopper la couverture en direct de manifestations antigouvernementales.

La diffusion de vidéo en temps réel est de plus en plus populaire depuis le lancement d'une appli désormais disparue, Meerkat, début 2015. De nombreuses applis ont depuis ajouté une fonction de streaming en direct et offrent leurs contenus sur un large réseau mondial. La possibilité de diffuser des images en direct depuis son appareil mobile sans avoir besoin d'équipement élaboré ou de stratégie de distribution a rendu cette technologie plus accessible. Les médias et autres producteurs de contenus continuent à diffuser des contenus en live depuis leurs propres sites web, parfois même en conjonction avec des applis et plateformes de réseau sociaux. Cela leur permet bien souvent de contourner les régulations spécifiques aux diffuseurs traditionnels, et d'atteindre de nouvelles audiences.

Les gens diffusent toutes sortes de choses, des évènements culturels aux interactions de la vie quotidienne. Cependant les vidéos en direct sont un excellent outil pour documenter les éventuels abus de l'état. En Arménie, le journaliste en ligne Davit Harutyunyan a signalé que des agents de police l'avaient attaqué et avaient cassé son équipement afin de l'empêcher de partager en direct des images de la police attaquant d'autres journalistes alors qu'ils couvraient des manifestations antigouvernementales. Même dans des démocraties comme les États-Unis, les outils de diffusion en direct sont devenus importants pour documenter les cas d'injustice sociale. Dans l'un des cas, la diffusion en direct d'une vidéo sur les réseaux sociaux par la petite amie de Philando Castile, un automobiliste afro-américain, après que la police l'ait abattu dans le Minnesota en Juillet 2016 a permis d'attirer l'attention de la nation entière sur cet évènement.

Les journalistes ont accueilli à bras ouverts le streaming en direct, qui est devenu une alternative, facile d'accès, à la diffusion sur chaînes de télé, surtout dans les pays où les médias traditionnels ne racontent pas l'histoire en entier. Avant les élections iraniennes de mai 2017, les personnalités réformistes qui soutenaient la quête du président Hassan Rouhani d'obtenir un second mandat utilisaient Instagram Live pour couvrir les évènements de la campagne et les programmes nocturnes malgré avoir été mis sur la touche par la société de diffusion nationale IRIB, qui a un monopole virtuel

sur la diffusion des médias traditionnels. Pour montrer le succès de cette stratégie, le protocole qui permet aux utilisateurs Instagram de diffuser des vidéos en direct fut momentanément bloqué, et quand il est redevenu accessible, le candidat Ebrahim Raisi s'en est lui aussi servi.

Les censeurs du gouvernement ont dû s'adapter aux tendances. Au Bahreïn, le ministère de l'information a interdit aux sites d'informations de diffuser des vidéos pendant tout juillet 2016. D'autres, comme lorsque l'Iran a bloqué Instagram, ont utilisé des méthodes pour stopper la diffusion en direct pendant qu'elle avait lieu. Au Venezuela, les fournisseurs de service ont reçu l'ordre de bloquer 3 sites web qui diffusaient en direct des dizaines de milliers de manifestants pour protester contre le président Maduro en Avril 2017. En Juin, la couverture en direct de manifestations anticorruption en Russie fut interrompue quand l'alimentation électrique du bureau du leader de l'opposition Aleksey Navalny fut intentionnellement coupée, laissant sa chaîne YouTube Navalny Live sans son et sans lumière.

L'utilisation par le public de smartphones pour documenter des évènements en temps réel a transformé des utilisateurs d'internet classiques en journalistes citoyens et donc en cibles pour le gouvernement. Au moins deux vloggeurs furent arrêtés et un troisième a dû payer une amende pour avoir diffusé des manifestations anti gouvernement en Biélorussie ; leurs collègues ont constaté un manque de soutien de la part des institutions et un manque de protection légale de leur profession. Une activiste des droits des animaux biélorusse a aussi eu une amende sous prétexte que sa vidéo en direct depuis un refuge d'animaux violait les lois sur les diffusions de médias de masse.

Le streaming en direct bénéficie d'une popularité croissante parce qu'il permet aux utilisateurs de diffuser en direct de la nudité, de la prise de drogue et de la violence. Certains pays ont restreint les diffusions en temps réel pour des questions de décence, mais les effets se sont étendus au journalisme et à l'activisme numérique. L'appli de streaming singapourienne Bigo Live a été fermée pendant un mois en Indonésie jusqu'à ce qu'ils parviennent à un accord avec le gouvernement, afin de limiter les activités de streaming qui viole l'interdiction indonésienne concernant les contenus obscènes ou « négatifs ». Et en Chine, la police de la province de Guangdong a clôturé des centaines de chaînes de streaming en direct lors d'une purge visant la pornographie et autres contenus illégaux.

Des cyberattaques touchent des sources d'informations, l'opposition, et des activistes des droits de l'homme

Une vague de cyberattaques extraordinaires a causé des perturbations significatives et des fuites de données cette année. Des millions d'appareils connectés non sécurisés comme des baby phones et machines à café furent piratés et utilisés pour frapper le

fournisseur de DNS Dyn d'une attaque DDoS, causant des coupures sur certaines des plateformes les plus populaires du net. Avec des motivations politiques de plus en plus intenses, des hackeurs ont également infiltré les serveurs du Comité national démocrate américain et la campagne des élections présidentielles du candidat français Emmanuel Macron en 2017.

Tandis que ces intrusions ont fait les gros titres, des attaques similaires ont touché des défenseurs des droits de l'homme, des membres de l'opposition, et des médias du monde entier à une fréquence plus importante que jamais, souvent avec la complicité de leurs propres gouvernements. Des attaques techniques contre les critiques du gouvernement ont été documentées dans 34 des 65 pays étudiés, contre 25 dans l'édition de 2016. Plutôt que de protéger les utilisateurs vulnérables, de nombreux gouvernements ont pris des mesures supplémentaires pour restreindre le cryptage, ce qui expose encore plus les citoyens.

Les problèmes de sécurité permettent aux affiliés du régime d'intimider les critiques et censurer la dissidence en ligne, sans avoir à assumer la responsabilité de leurs actes. Il est souvent difficile d'identifier les responsables de cyberattaques anonymes, surtout quand c'est le gouvernement qui est soupçonné. La Chine, l'Éthiopie, l'Iran, et la Syrie sont les plus gros producteurs de ce type d'attaque, mais le marché dynamique et peu régulé de cyber outils de qualité militaire a baissé le coût de telles activités. Même les autorités policières locales peuvent désormais persécuter leurs « ennemis » avec peu de surveillance. D'ailleurs, les attaques techniques représentent actuellement la forme de contrôle la plus commune observée par Freedom House, derrière les arrestations d'utilisateurs pour avoir publié du contenu.

Les activistes et les organes de presse ont souvent des défenses limitées contre les attaques techniques, ce qui peut causer de la censure, de la surveillance, de la manipulation de contenu et de l'intimidation. De nombreuses attaques ne sont pas signalées, surtout quand il n'existe aucun moyen de le faire ou quand les victimes craignent les représailles.

Un protestataire à une manifestation à Moscou, en août 2017, contre l'augmentation de la surveillance du gouvernement et des restrictions sur internet.
(Credit MAXIM ZMEYEV/AFP/Getty Images)

Des sites indépendants sont temporairement désactivés

Les activistes et les organes de presse d'au moins 18 pays ont signalé des interruptions de service causées par des cyberattaques, surtout des attaques de type DDoS, durant lesquelles plusieurs requêtes simultanées de nombreux ordinateurs surchargent et désactivent un site ou système. Ces types d'attaques sont devenus un moyen facile et peu onéreux de se venger de ceux qui parlent de sujets sensibles.

L'Eurasie et l'Amérique latine sont les régions où il y a eu le plus d'attaques réussies. En Azerbaïdjan, la plateforme en ligne indépendante d'informations *Abzas* a signalé avoir subi une série d'attaque DDoS qui a duré plusieurs jours en janvier 2017. Le site était inaccessible jusqu'à ce qu'il migre vers un hébergeur plus sécurisé. Une enquête a relié les adresses IP qui ont lancé l'attaque à plusieurs institutions gouvernementales Azerbaidjanaises. La presse et les organisations sociales civiles du Venezuela ont remarqué une augmentation du nombres d'attaques début 2017. Comme par exemple

une attaque contre Acción Solidaria, une organisation qui aide les gens qui vivent avec le HIV. La perturbation a temporairement empêché le groupe d'informer les utilisateurs des distributions de médicaments.

Le piratage informatique permet la surveillance des reporters et des dissidents

Des victimes se sont fait voler leurs appareils ou encore pirater leurs comptes pour des motifs politiques dans au moins 17 pays. La menace de surveillance peut avoir un effet intense sur le travail des journalistes, des défenseurs des droits de l'homme et des activistes politiques d'opposition, précisément visés ces dernières années.

Des campagnes de phishing à grande échelle comme « Nile Phish » en Égypte ont tenté d'obtenir des informations sensibles chez des organisations de défense des droits de l'homme avec des emails trompeurs. Aux Émirats Arabes Unis (EAU), des spywares développés par la firme israélienne NSO—qui déclare ne vendre cette technologie qu'aux autorités policières et organisations de renseignements—furent utilisés contre le défenseur des droits de l'homme Ahmed Mansoor, faisant écho à de précédents rapports à propos de contrats gouvernementaux avec l'entreprise italienne Hacking Team afin de surveiller certains activistes.

Le spyware de la NSO a également été utilisé contre des journalistes mexicains connus, des avocats des droits de l'homme et des activistes, qui ont reçu des messages hautement personnalisés et souvent très effrayants. L'une des nombreuses cibles était un avocat représentant les parents de 43 étudiants manifestants, disparus en 2014. Quelques jours après avoir cliqué sur un lien dans un sms qui lui demandait son aide, un enregistrement d'un appel entre lui et un des parents a fait surface en ligne.

Les lois sur le cryptage ouvrent les portes aux abus

Plutôt que de prendre des mesures pour protéger les entreprises, les citoyens et les groupes de gens vulnérables contre ces menaces de cyber sécurité, de nombreux gouvernements prennent la direction opposée.

Les restrictions sur le cryptage ont continué à augmenter, poursuivant la tendance observée par *La liberté du Net* depuis plusieurs années. Au moins six pays, la Chine, la Hongrie, la Russie, la Thaïlande, le Royaume-Uni et le Vietnam ont récemment voté des lois qui peuvent exiger des entreprises ou des individus qu'ils décryptent du contenu, donnant ainsi un accès à des communications confidentielles.

Le cryptage mélange les données afin qu'elles ne puissent être lues que par le destinataire prévu, offrant une protection supplémentaire aux activistes et journalistes qui ont besoin de communiquer de manière sécurisée. Mais même les gouvernements démocratiques le perçoivent comme un simple outil de protection des terroristes et autres criminels contre les autorités policières.

Les pays européens ont été rapides à créer des lois à la suite des attaques terroristes, introduisant des mesures pouvant compromettre la sécurité de tout le monde. Des lois anti-terrorisme ont été votées en Hongrie en Juillet 2016 obligeant les fournisseurs de services de cryptage à autoriser l'accès aux autorités aux communications de leurs clients. Le Investigatory Powers Act du Royaume-Uni, voté en Novembre 2016, pourrait être utilisé pour forcer les entreprises à supprimer la « protection électronique » des communications ou des données quand c'est techniquement faisable. « Les gens normaux préfèrent souvent la facilité d'utilisation… à la sécurité parfaite et incontournable » a déclaré la secrétaire d'état Amber Rudd en Juillet 2017. Mais David Kaye a déclaré que le cryptage et que l'anonymat étaient essentiels à la liberté d'expression et au droit à la confidentialité.

D'autres gouvernements ont cité des raisons de cyber sécurité et de lutte contre le terrorisme pour justifier des mesures qui leur permettent de surveiller des activistes et des journalistes dans un contexte de répression. De récents amendements aux lois informatiques de Thaïlande qui pourraient forcer les fournisseurs de service à « décoder » des données informatiques sont particulièrement inquiétants. Privacy International a dénoncé Microsoft pour avoir utilisé les certificats racines nationaux par défaut, permettant potentiellement à l'état militaire de falsifier des identifiants sur des sites, enregistrer les identifiants des utilisateurs, et décrypter des connexions. Des inquiétudes semblables ont fait surface dans le passé avec les certificats racines chinois et les abus potentiels qui pouvaient en découler. Dans des pays répressifs comme ceux-là, les messages privés sont souvent utilisés pour poursuivre en justice les critiques du gouvernement. Un tribunal militaire thaïlandais a condamné un activiste politique à plus de 11 ans de prison en Janvier 2017 en se basant sur des retranscriptions de messages censés provenir d'un échange privé sur Messenger.

Il est dur de savoir comment les intermédiaires appliqueront les demandes de décryptage des communications en pratique, surtout dans le cas de cryptages d'un bout à l'autre, lors duquel des clés de décryptage sont sur les appareils des utilisateurs plutôt que sur les serveurs d'une entreprise. Un niveau de connaissances informatiques faible chez les législateurs se traduit souvent par des lois problématiques, à la fois en termes de droits humains mais aussi de mise en place. Au Kazakhstan, par exemple, des actions pour permettre au gouvernement de surveiller le trafic crypté avec un « certificat de sécurité national » ont été mises au placard quand les autorités ont réalisé le côté inapplicable de cette loi.

De nouveaux outils de cyber sécurité donnent de l'espoir

Malgré ces régulations souvent problématiques de la part des gouvernements, des entreprises privées tentent d'offrir aux clients des mesures de sécurité améliorées. Google a fait part de ses intentions de déployer des protections supplémentaires contre les attaque "man-in-the-middle" sur son navigateur web Chrome. Comme Facebook, Microsoft, Twitter, et d'autres, l'entreprise a également averti ses utilisateurs qu'elle soupçonnait être victimes d'attaque de hackeurs sponsorisés par l'état.

Si une protection peut coûter cher, certaines initiatives privées proposent une protection gratuite pour les organes de presse et les sites de défense des droits de l'homme avec des moyens limités. Les exemples incluent Project Shield (Google), Project Galileo (Cloudflare), et Deflect. Dans l'un des cas, Project Shield a aidé le site d'informations indépendant Angolais *Maka Angola* à se défendre contre une attaque DDoS.

De tels services peuvent aider à combattre certain types d'attaques, mais les organisations civiles et les organes de presse indépendants ont encore du mal à gérer l'abondance de tactiques utilisées par leurs adversaires sur le cyber espace, sans parler de parvenir à attirer l'attention sur ces menaces et les empêcher.

L'utilisation des VPN augmente, de même que leurs restrictions

Les VPN dirigent toutes les connexions d'un utilisateur sur un serveur à distance, permettant l'accès à des contenus à restrictions géographiques, et certains d'entre eux cryptent ou masquent l'activité des utilisateurs de leur fournisseurs d'accès (FAI). Six pays, la Biélorussie, la Chine, l'Égypte, la Russie, la Turquie et les EAU ont pris des mesures pour contrôler ces outils l'année passée, soit en publiant des lois qui interdisent de contourner la censure, soit en bloquant des sites web ou du trafic réseau associé aux VPN. De telles répressions suivent souvent des périodes de censures agressives qui forcent les utilisateurs à chercher des moyens de contourner la restriction de l'information. Le gouvernement égyptien, qui a commencé à bloquer des sites d'information indépendants pour la première fois en Décembre 2015, a censuré au moins cinq sites proposant des VPN en 2017.

Les campagnes contre les VPN sont impopulaires et difficiles à mettre en place. De nombreuses personnes dépendent des VPN pour plusieurs choses, comme par exemple des employés d'entreprise souhaitant accéder à des fichiers sur des serveurs à distance, ou des utilisateurs internet soucieux de leur sécurité lors d'une connexion à un réseau wifi public. Dans les pays qui bloquent les informations internationales, les scientifiques et économistes locaux, et même certains officiels du gouvernement comptent sur les VPN pour rester informés.

C’est pour cette raison qu’aucun pays n’a encore totalement banni les VPN. À la place, les états les plus répressifs vont vers un système à deux niveaux, qui autoriserait certains VPN pour des usages approuvés et bannirait le reste. Même si le trafic VPN se révèle impossible à réguler complètement, les états peuvent pousser les utilisateurs vers les fournisseurs plus susceptibles de coopérer avec les autorités policières locales et créer des lois pour pénaliser ceux qui se font attraper à utiliser une connexion sécurisée pour les mauvaises raisons.

Les autorités chinoises ont voté une série de lois l’année dernière, pour doter les fournisseurs de VPN d’une licence, et demander aux FAI de bloquer ceux qui ne possédaient pas de licence ; en juillet 2017, Apple a informé plusieurs opérateurs de VPN que leurs applis n’étaient plus accessibles par l’app store chinois de l’entreprise pour cause de non-respect des lois. Aux EAU, les internautes et les entreprises se sont dépêchés de comprendre les implications des nouveaux amendements de la loi sur la cyber criminalité, qui recommandaient de lourdes amendes et de possibles peines de prison en cas d’utilisation d’un VPN pour commettre des fraudes et des crimes. La Russie a également passé une loi qui oblige les FAI à bloquer les sites web qui proposent des VPN qui peuvent être utilisés pour accéder à du contenu banni ; les autorités russes ont perquisitionné les bureaux et les serveurs appartenant à un fournisseur de VPN étranger, Private Internet Access, en 2016. Des VPN ont été temporairement restreints dans au moins neuf autres pays, y compris l’Iran, ou les autorités ont apparemment créé un outil VPN qui permet à ses utilisateurs d’accéder à des contenus bannis mais dont toutes les activités sont surveillées par l’état.

Certains VPN sont plus durs à surveiller et à bloquer, avec des protocoles de sécurité plus solides et des politiques strictes contre la divulgation de données. Mais les gouvernements répressifs visent tout spécialement les outils les plus sûrs. Tor, un projet qui crypte et rend le trafic web anonyme en le routant à travers un réseau complexe d’ordinateurs volontaires, a été sujet à de nouveaux blocages et censures en Biélorussie, Turquie et Égypte. Les ordres de blocage peuvent concerner le site où les utilisateurs téléchargent les logiciels nécessaires pour accéder au réseau Tor, ou pour accéder au trafic des ordinateurs qui constituent le réseau. De telles mesures ne vont pas éradiquer Tor, mais cela rend l’accès plus difficile pour la population. Les utilisateurs qui n’ont pas pu atteindre le site l’année passée ont continué à partager des options de téléchargement du logiciel par email, mais il faut savoir à qui demander.

Les attaques physiques sur les internautes et les journalistes en ligne se répandent dans le monde entier

Des attaques physiques en représailles d’activités en ligne ont été signalées dans 30 pays, contre 20 dans l’édition 2016 de *La liberté du Net*. Dans huit pays, des gens ont

été assassinés pour avoir parlé de sujets sensibles en ligne. Et dans quatre de ces pays —le Brésil, le Mexique, le Pakistan, et la Syrie— de tels meurtres ont eu lieu tous les ans ces trois dernières années. Les cibles les plus fréquentes semblent être les journalistes en ligne et les bloggeurs parlant de politique, de corruption et de crime, mais également les gens exprimant leurs opinions religieuses, qui tranchent avec celles en place. Dans la plupart des cas, les coupables restent anonymes, mais ces actions sont souvent en relation directe avec les intérêts d'individus ou d'entités politiques puissants.

La violence physique est une tactique de censure cruelle mais efficace, surtout dans les pays où des sites connus fournissent un moyen pour les reportages d'investigation indépendants d'être publiés, et où les médias traditionnels sont souvent affiliés au gouvernement. Pavel Sheremet, un journaliste d'investigation du site ukrainien *Ukrayinska Pravda*, est décédé à cause d'une bombe cachée dans sa voiture à Kiev en Juillet 2016. Un an plus tard, le meurtre reste irrésolu, et les journalistes locaux ont divulgué de sérieuses failles dans l'enquête menée par les autorités ukrainiennes.

Dans certains pays, les journalistes utilisent des chaines de réseaux sociaux officieuses pour publier leur travail ou le détailler et s'attirent des représailles. Soe Moe Tun, un journaliste de presse écrite chez le *Daily Eleven* de Myanmar, fut battu à mort moins d'une semaine après avoir publié des images de ses carnets sur Facebook. Les notes donnaient les noms d'individus ayant participé à un abattage d'arbres illégal dans la région de Sagaing.

Dans plusieurs cas signalés, les assaillants ont cherché à retirer du contenu en ligne. Gertrude Uwitware, une journaliste en Ouganda, fut kidnappée pendant huit heures en Avril 2017 par des inconnus. Ils lui ont ordonné de supprimer ses publications sur des réseaux sociaux où elle exprimait son soutien pour un chercheur mis en prison le même mois pour avoir appelé le président Yoweri Museveni « une paire de fesses » en ligne.

Les groupes religieux s'adaptent eux aussi à internet, et les opinions qu'on partage avec une poignée de proches sont dorénavant plus susceptibles d'attirer l'attention d'extrémistes qui surveillent les réseaux sociaux à la recherche d'occasions de punir les dissidents. Au Pakistan, où un tribunal a condamné un utilisateur d'internet à mort pour avoir commis un blasphème sur Facebook, un étudiant de la province de Khyber Pakhtunkhwa a été assassiné sur le campus par la foule, qui l'accusait d'avoir posté des contenus blasphématoires en ligne. En Septembre 2016, l'auteur chrétien Nahed Hattar a été assassiné par balle devant un tribunal en Jordanie, où il était jugé pour avoir insulté l'Islam sur Facebook avec un dessin parodiant la vision du paradis des terroristes. De telles attaques réussissent souvent à faire taire bien plus que la victime, étant donné qu'elles encouragent à encore plus d'auto censure sur les sujets sensibles tels que la religion.

L'échec de l'état à punir les coupables des représailles pour s'être exprimé en ligne perpétue un cycle d'impunité. Mais le rôle nocif du gouvernement a été encore plus

direct dans sept pays, où des individus détenus à cause de leurs activités en ligne ont signalé avoir été victimes de tortures. Ces pays incluent le Bahreïn, où l'activiste des droits de l'homme Ebtisam al-Saegh déclare avoir été agressée sexuellement par des agents de sécurité après son arrestation en Mai 2017 pour avoir critiqué l'état sur Twitter.

Sujets censurés par pays

La censure est présente si l'état bloque ou ordonne le retrait de contenu, détient ou verbalise les utilisateurs pour avoir posté des contenus concernant certains sujets. Le graphique ne tient pas compte des pressions telles que la violence, l'autocensure, les cyberattaques, même si c'est l'état qui est soupçonné.

vpnMentor a collaboré avec le rapport Freedom on the Net 2017 de la Freedom House, afin de le traduire en français et informé les francophones du monde entier de l'état des libertés en ligne en 2017.